Betere zorg
door betere informatie

Nictiz

Patient safety versus new Privacy Regulations

Anton Ekker

HIMSS, November 6 2014

Privacy versus patient safety

- Current legal developments regarding electronic processing of medical data:
  - Dutch proposal on patient rights;
  - verification of treatment relation: findings of DDPA;
  - GDPR: right to erasure

I: Proposal on patient rights

- applicable to systems for electronic data exchange between healthcare professionals
- specific consent for making available all or specific data to (categories of) health care providers, to be determined by the patient:
  - how to define and identify ‘categories’?
  - relation to existing authorization policies;
  - standardization is needed!
- consent for consulting data within ‘treatment relation’

- exception for access to information in emergency situations: does ‘breaking the glass’ make health care professionals hesitant to consult medical data?

- in case new categories of health care providers are included, or the functionality of the data exchange is substantially modified, the health care provider should inform the patient about:

  - the modification
  - the possibility to withdraw or modify his consent

II: Treatment relation

Relation between patient and healthcare provider that:

- has a treatment contract;
- is directly involved or,
- acts as a substitute

DDPA: verification required

- DDPA: verification is legally required
- role based access control / context is not sufficient: treatment relation must be established with certainty prior to authorisation
- research on 9 healthcare institutions: none of them were compliant

Betere zorg
door betere informatie Nictiz

III: GDPR: right to erasure

Article 17 GDPR

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of, that data where one of the following grounds applies:

   […]

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

   (c) the data subject objects to the processing of personal data pursuant to Article 19;

3. The controller and, where applicable, the third party shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(b) for reasons of public interest in the area of public health in accordance with Article 81;

9. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

Questions?

ekker@nictiz.nl
06-43775335